Spring 5-18-2015

Mobile Device Use: Increasing Privacy and Security Awareness for Nurse Practitioners

Lauren Storbrauck
La Salle University, storbrauckl1@student.lasalle.edu

Mobile Device Use:
Increasing Privacy and Security Awareness for Nurse Practitioners

By: Lauren Storbrauck

La Salle University

Economic Crime Forensics- Network Security Track

April 30, 2015

Table of Contents

Abstract

Nurse practitioners are increasingly using mobile devices to access electronic medical records, as the use of the devices increases so does the risk of a potential breach. This is a direct result of technological advances such as larger storage capacities, faster computing speeds, and better portability/connectivity (Torrieri, 2011). These devices include: mobile phones, tablets, and laptops. The use of these devices has greatly facilitated the work of Nurse Practitioners, by allowing them to have instant access to patient records, health history and recommended treatment plans (Ventola, 2014). However, seventy-three percent of all mobile users stated that they are not always aware of security threats or best practices when working with mobile devices (Hickey, 2007). It is important for healthcare organizations to have in place policies and procedures, and processes for mobile device use and to educate their employees on these topics (Kolbasuk, 2011). Increased security knowledge is a direct result of training (Fisher, 2015).

The purpose of this project is to identify the risks associated with mobile device use by Nurse Practitioners, discuss the relevant laws, and provide an overview of relevant cases. Then, the project will create a framework consisting of a Standard Operating Procedure, mobile device privacy and security educational power point, and post education knowledge assessment questionnaire. The training will focus on the importance of developing best practices, including developing strong passwords, enabling encryption, keeping security software up to date, and maintaining physical control of the device at all times. In addition, to create a security culture where the Nurse Practitioners receive annual training on securing Protected Health Information, or PHI, on their mobile devices.

Introduction

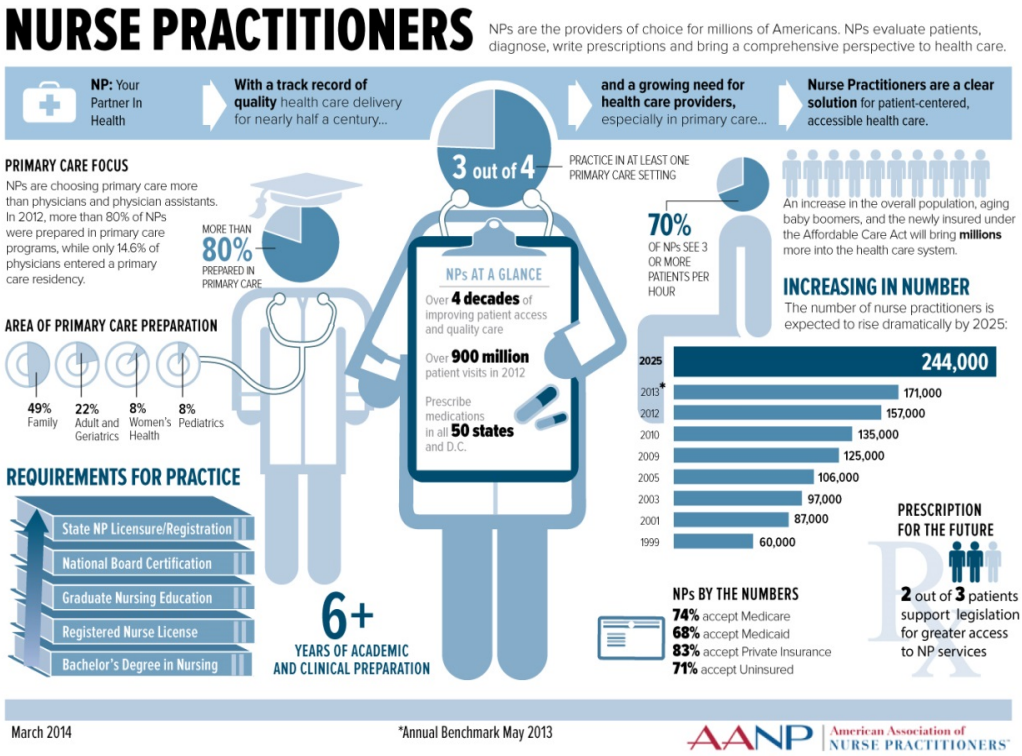
Mobile devices (laptops, smartphones, and tablets) are transforming the healthcare profession (Ventola, 2014). Among healthcare professionals, Nurse Practitioners are considered "shining stars" in relation to mobile device engagement. They are second, only to physician's assistants in "daily tablet usage" (Epocrates, 2014). They use these devices to access, transmit, receive and store personal health information. Between 2012 and 2013, there was a 68% increase in 'digital omnivores', or those using three devices (Walker, 2014). The continued growth in the use of mobile devices by Nurse Practitioners can be attributed to their portability, relative ease of use and convenience. Mobile devices allow Nurse Practitioners the ability to easily travel from patient to patient without being confined to a desk, which is essential to performing their job. Mobility and portability allow the provider the opportunity to complete a health visit in the patient's home, clinic or skilled facility and still have access to the patient's medical records. Also, it allows them to send lab requests, and prescriptions to the pharmacy. Therefore, potential security threats continue to grow with increased use and enhanced provider training is key to raising awareness to potential threats.

Risk Assessment

Figure 1 illustrates why it is so important to focus on Nurse Practitioners. The profession is growing at an unprecedented rate. The number of practicing Nurse Practitioners is expected to rise to an all-time high by 2025 to 244,000. Nurse Practitioners have a masters or doctoral level of education and perform similar tasks to their physician counterparts. The completion of masters/doctoral level education is a requirement that varies depending on their board certifying agencies (ANCC, AANP). Healthcare companies hire Nurse Practitioners to provide medical

care as well as provide onsite case management assistance. A majority of Nurse Practitioners practice within at least one primary care facility and see three or more patients per hour. This means that at any given point, a Nurse Practitioner has access to dozens of medical records on their devices on a daily basis. They are often using their organization's provided devices in the field, at nurse stations, in waiting rooms or in other public locations. This puts them at a greater risk for unauthorized access to information as well as loss or theft. In responding to an urgent issue with a patient, they may inadvertently leave their medical devices unattended.

Figure 1



Source: American Association for Nurse Practitioners, 2014

Mobile devices have revolutionized the way Nurse Practitioners conduct their job, however despite these benefits, mobile devices also pose a significant risk to the protection of PHI. These risks include unauthorized access if the device is lost and/or stolen (McCarthy, 2014). PHI may be located on the SIM card of a smartphone or tablet or in the memory of a laptop computer. This stored PHI makes them valuable targets for thieves. If the device does not have sufficient security measures in place (e.g. strong encryption and access controls) once the thief has the device s/he can find the PHI stored on the SIM card and sell it on the black market. Due to their small, portable size mobile devices are particularly vulnerable to being lost or stolen. The most common breach of PHI (about 68%), is due to the theft of a mobile device (McCarthy, 2014).

However this is not the only way information may be stolen from a device. Another way, thieves may access the device occurs when a Nurse Practitioner connects to an unsecure Wi-Fi network. An unsecure network is a system that has no password or login credentials. These unsecure networks are very common especially in bookstores, coffee shops, and hotels. To understand the danger of the "free public Wi-Fi" networks it is important to understand the two types of Wi-Fi networks that are commonly used: traditional access point networks and Ad-hoc networks. Ad-hoc networks connect devices directly to another device; this is dissimilar to traditional access point networks which connect directly to a central router.

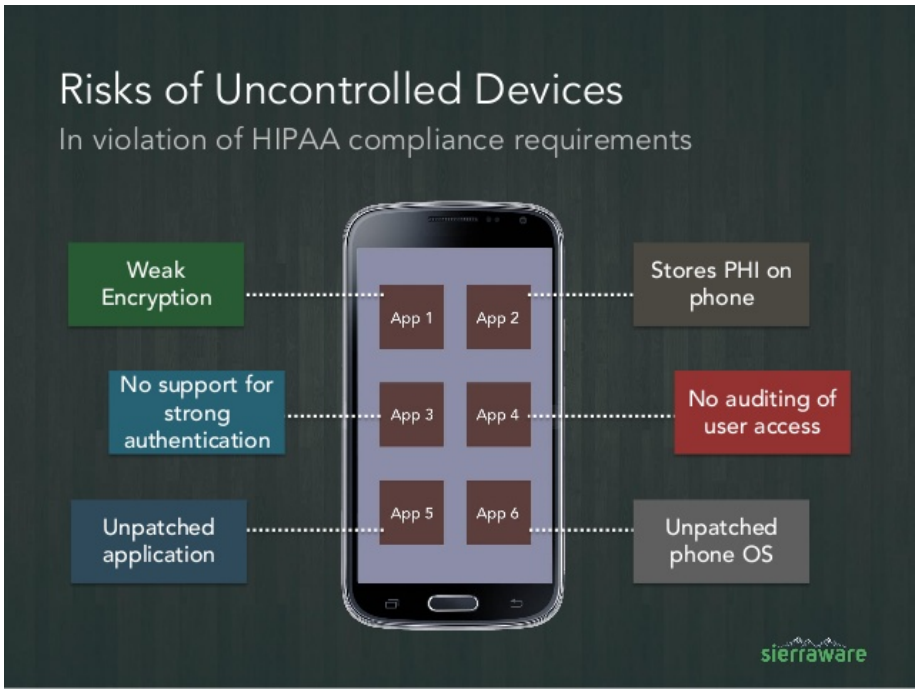
Simply put, when connecting to an ad-hoc network the user is connecting to another device and from there the user's device will then be set up to broadcast the "free public Wi-Fi" network to other devices in the area (Escobar 2013). Through this interconnected web of devices a hacker can sit on the network and locate your device. The lack of authentication gives a hacker unfettered access to the network. If the hacker positions himself between the Nurse Practitioner's

device and the connection point. The Nurse Practitioner may be sending PHI directly to the hacker. From here, the hacker can open, view and download information on your mobile device (Torrieri, 2011). These ad-hoc networks do not have the same security measures in place. Any information from a patient's health record could be compromised over an unsecure public network.

This is one of the many examples of how a device is only as safe as the awareness and understanding of the user who holds it. Breaches in PHI have become an unfortunate side effect of mobile device use; the Department of Health and Human Services reported that 81,790 breaches of patient information occurred as of January 1, 2013 as a result of using mobile devices (McDavid, 2015). Cyber criminals can access mobile devices using phishing e-mail, spam, spyware, malware, use the information for financial gain or to commit electronic fraud, identity theft, or extortion. These cyber criminals may attack mobile devices for a large-scale financial gain or intellectual property theft (Kolbasuk, 2011).

Figure 2 highlights some of the risks associated with using devices that are not properly monitored. Weak encryption, lack of strong authentication, failure to update OS regularly, and lack of auditing controls are just some of these risky behaviors.

Figure 2



Sierraware, 2014

Weak encryption, and authentication protocols make the PHI stored on devices susceptible to unauthorized access. Without strong encryption and password protection, if the device were lost or stolen, the thief could access the device with ease. Nurse Practitioners need to be aware not only of potential security flaws in these mobile devices but in the way they use these devices. Having no password, using weak passwords like 1234, or sharing login credentials are a few of the ways a Nurse Practitioner may misuse his/her device. They need to take the steps necessary to patch these vulnerabilities or they may find themselves in violation of the law. Most providers are not aware of the importance of protecting the privacy and security of patient information. Failure to protect this information can result in legal repercussions as well as heavy fines.

The goal of this project is to raise awareness of the various threats and risks of mobile device use by Nurse Practitioners, and develop an educational training program to mitigate these risks. All staff on an annual basis will attend the program, and new hires will immediately complete this training prior to using corporate mobile devices. The policy and procedure developed will be used as the basis for the training session. The post-training questionnaire would assess knowledge gained with a minimal score of 80% needed to successfully complete the training session. All learners will need to sign off that they have completed the training session and will comply with all corporate policies and procedures related to mobile device use. The Director will ensure the training is completed on an annual basis by all Nurse Practitioners and continue to create a culture of security threat awareness by staff.

2015 Policy and Procedure Development and Training

Law

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

In addition to policies and procedure established by their employers, Nurse Practitioners are required to comply with federal law. In an attempt to secure patient information, the United States Government enacted, the Health Insurance Portability and Accountability Act, known as HIPAA, on August 21, 1996, which sets the national standards for protected health information and mobile use (Taitsman, 2013). HIPAA protects the confidentiality, integrity and availability of electronic PHI. The law defines mobile devices as smartphones, laptops or tablets and it acknowledges the important role they play in healthcare. Under HIPAA, PHI includes demographic data that relates to: the individual's past, present or future physical or mental health and/or condition. PHI can also include payments made for the provision of health care and

includes the patient's name, address, birthdate and social security number. According to HIPAA, healthcare providers who are considered covered entities are required to secure their patients' PHI whether stored on paper or in digital form. Failure to comply with HIPAA, can result in civil penalties of $50,000 per violation and criminal penalties resulting in a $250,000 fine with imprisonment up to 10 years (Tynan, 2011). These large penalties and fines are meant to send a loud message that security of PHI is a top priority.

In response to the increased use of the Internet and mobile devices in the early 2000s, Congress added the Security rule to HIPAA. Effective April 21, 2003, the Security Act was added, to affirm and elaborate on "standards for the security of electronic protected health information…. [by] establishing a level of protection" (Federal Register, 2003). Covered entities must safeguard the confidentiality of integrity and availability of its PHI. It requires healthcare professionals to meet administrative, physical, and technical requirements to protect PHI (Barrett, 2011).

The law requires that certain safeguards to protect PHI be implemented, these safeguards include but are not limited to: ensuring secure passwords are in place, using strong encryption, enabling remote wipe, installing a good firewall, and using secure Wi-Fi connections (Taitsman, 2013). Federal regulations and state laws are in place to help secure patient electronic medical records and to guide the adoption of health information technology (HHS, 2013).

In a survey conducted by NueMD in conjunction with Porter Research, The Daniel Brown Law Group found that there is a lack in HIPAA compliance knowledge on mobile device use. Only 35% of participants (which included Nurse Practitioner and other clinicians) responded that they have conducted the HIPAA required risk analysis. Attorney Matt Fisher reiterated the NueMD's findings, stating that "comprehensive HIPAA training" should be

required and suggested the primary focus of this training concentrate on mobile devices. Most importantly Fisher stated, that "training cannot be overlooked…do not allow a violation to occur because of a lack of training: knowledge is power" (Fisher, 2015). This survey further supports the need for comprehensive mobile device security training for all Nurse Practitioners. All organizations should educate employees about security policies, procedures, and processes for devices, networks and people (Kolbasuk, 2011).

HITECH

The Health Information Technology for Economic and Clinical Health Act (HITECH) widened the privacy and security provisions in HIPAA. It mandates the notification of victims in the event of a breach of PHI that is held by HIPAA covered entities and vendors (Taitsman, 2013). Providers and insurance companies are now responsible to notify patients if PHI may have been compromised. This is an effort by the government to make the security and privacy of patient's medical records a priority. Also, the act gives patients the opportunity to work with their providers to protect data and maintain privacy, and outlines the importance of prompt notification is a potential breach has taken place.

Cases

Hospice of Northern Idaho

Breaches of PHI caused by mobile devices are far from infrequent. The Journal of Medical Practice Management acknowledges that most "providers will experience one or more information breaches" (McDavid, 2015). Recently, the U.S. Department of Health and Human Services (HHS) investigated the Hospice of Northern Idaho for an alleged violation of HIPAA,

in which the breach resulted in the electronic PHI of 441 patients being compromised. The breach occurred as a result of an unencrypted laptop being stolen. The Journal of Geriatric Nursing, highlighted this breach in their March 2013 issue, stating that, "critical to its analysis of how to respond to the breach were findings that the hospice provider: failed to conduct a risk analysis to safeguard the electronic PHI stored on its laptop and failed to implement company policies to address the risks posed by mobile device security" (Senft, 2013).

The recommendation provided by the Geriatric Nursing Journal to prevent another breach was to encourage health care professionals to partake in educational training on mobile devices. Comprehensive training will ensure that they have the knowledge to safely and responsibly use these devices, without risk of violating the law or compromising a patient's health information. Security professionals are unanimous that the weakest link in any computer system is the user (Healthit.gov, 2013).

Concentra Health

One of the largest settlements related to a PHI breech was levied against Concentra Health Service, a subsidiary of Humana. Concentra was required to pay $1.7 million for violating HIPAA (Mangan, 2014). The settlement came after the Department of Health and Human Service's Office for Civil Rights conducted a compliance review audit after a report that an unencrypted laptop had been stolen from one of their facilities. This laptop contained PHI of 148 patients. The report from the Office for Civil Rights found that Concentra was aware of the lack of encryption on its mobile devices, and understood the risks to PHI. In the corrective action plan, which Concentra agreed to in its settlement, they are required to encrypt all existing

computers, and to create a plan for encrypting new computers promptly (Mangan, 2014). In addition, corrective action plan requires that within,

> 120 days of the Effective Date, at one year following the Effective Date, and at the conclusion of the one year period thereafter, Concentra shall provide documentation to indicate that all workforce members have completed security awareness training (to include training on Concentra's Acceptable Use Policy), which shall also include all training materials used for the training, a summary of the topics covered (Concentra Resolution Agreement 2014).

The Department of Health and Human Services identified in this case a fundamental need for Concentra to train their employees on security awareness and to perform this training on an annual basis.

Approach

Privacy and Awareness Training Implementation

The cases highlight the lack of education surrounding how to be HIPAA/HITECH compliant with PHI when using mobile devices. The Journal of Medical Practice Management, recommend "an ongoing education program for HIPAA privacy and security" for Nurse Practitioners accessing PHI through mobile device. The Journal of Medical Practice Management identifies, "prevention as the optimum strategy" (McDavid, 2015). From the cases previously discussed and the problem areas that have been identified on which the Standard Operating Procedure, and training program will focus. These include: access controls, and encryption. These problems will be addressed by implementing a training program. The training program focuses on best practices for Nurse Practitioners to utilize, these include access controls

(setting strong passwords and not sharing their unique identification information), encryption methods, and never using an unsecured website. The training was developed from a comprehensive review of the literature, the law and the policy and procedure.

Access Controls

Part of the requirements mandated by HIPAA, is that Nurse Practitioners must utilize access controls. Access is "the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource" (HIPAA Security Series 2007). Access controls grant rights and privileges to access and utilize information, programs and files. The purpose of introducing access controls is to prevent unauthorized individuals from viewing PHI. The access control standard required by the Security Rule in HIPAA recommends several controls: unique user identification (required), automatic logoff (recommended) and encryption (recommended).

Unique user identification is a way to identify a particular user by name or by number. Both allows a user's activity to be tracked when logged into the system and holds them accountable for their actions. If there is a leak in PHI a system administrator should be able to track the breach to a unique user identification number, which could be tied to the individual. Whereas the organization is responsible for providing the login information to the Nurse Practitioner, the Nurse Practitioner is responsible for remembering their unique user identification, utilizing a strong password and protecting their user information from disclosure. A Nurse Practitioner should never allow another individual to use their unique user identification and password.

Automatic logoff is one of the simplest ways to protect PHI. It is a safeguard recommended by HIPAA. The purpose of automatic logoff is to terminate electronic sessions after a certain amount of time has passed without activity from the user. This safeguard is important no matter where the Nurse Practitioner is working because it prevents unauthorized individuals from using/ viewing the information on the device. For example if a Nurse Practitioner is working in a coffee shop and they walk away from their device, after a period of time the device should log them out so that when they return they would need to re-enter their unique user identification and password again. This prevents an unauthorized user from accessing the device and its information while the Nurse Practitioner is away.

Encryption

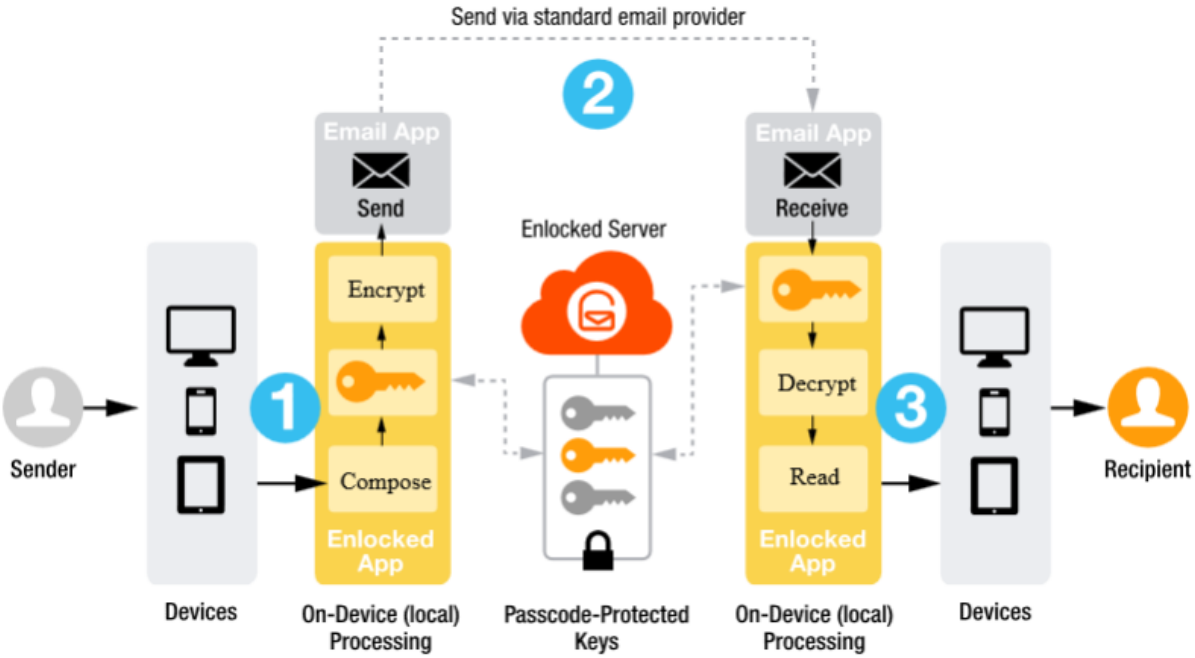
The encryption of PHI is a safeguard required under the security rule of HIPAA. It is the use of an "algorithmic process to transform data into a form which there us a low probability of assigning meaning without use of a confidential process or key" (HIPAA). There are three main areas of encryption: first, the privacy of communication, second, privacy of storage and third, forward secrecy. Forward secrecy is the protection of information regardless of the age of the information. All three of these areas pertains to the security of PHI on mobile devices.

In both the cases of the Hospice of Northern Idaho and Concentra, the encryption of data on a mobile devices could have prevented the breach in PHI. Part of the training program will include teaching Nurse Practitioners what encryption is, how it works and why it's important. Figure 3 shows one of the ways communications between devices can be encrypted.

Figure 3 depicts how public and private key encryption works. In this image a user is trying to send an email from their mobile device to the recipient's mobile device. This figure

shows how Enlocked, Inc. encrypts email messages. First when you download the Enlocked, Inc. application you are prompted to create a password which allows you to create and access your private key, which is a cryptographic key comprised of a string of random numbers. When sending a message the sender encrypts the e-mail locally on the device with the recipient's public key. This key, which is housed in a publically accessible repository is mathematically related to the recipient's private key. The message can only be decrypted by the recipient's private key. This is known as end-to-end encryption. The benefit of an application like this is that it works behind the scene, using the recipient's public key to encrypt the message.

Figure 3



Source: Enlocked, inc., 2014

Strategies for Determining Success

The Standard Operating Procedure

To minimize the problems surrounding mobile devices and securing PHI, Appendix A, B and C offer an organization policies and procedures to be implemented, an educational program and strategies for determining the success of the program. These appendixes have been developed through studying the applicable law and identifying the risks presented in the cases highlighted above. Appendix A is a Standard Operating Procedure (SOP) template for healthcare organizations to implement. It is important that the first step an organization takes to make themselves compliant with HIPAA and HITECH is to set in place the policies and procedures that Nurse Practitioners are expected to be compliant with. Appendix A offers a framework for healthcare organizations to implement that can be specifically tailored to it's individual needs and operations.

The SOP begins with setting up access control for employees. Here, management should work with IT to establish the level of access employees need to do their job. This serves two purposes: first, it eliminates some of the risks associated with unauthorized access by limiting it to only those who need it and second it gives assess to only the devices an employee needs. Next the SOP establishes the general security requirement. This policy requires that employees be provided with authentication credentials (i.e. usernames and passwords). This prevents unauthorized access and allows IT to track a user through the system to see when they have accessed their mobile device and what information they have accessed. The username and password given to an employee is associated with the level of access that employee needs and it is not to be shared. Nurse Practitioner's mobile devices are required to be encrypted and communications related to PHI from the mobile device should also be encrypted.

Next, the SOP recommends certain measures including using only secured Wi-Fi, a privacy screen and automatic logoff when out in public and locking the device when not in use. The user must notify their supervisor in the event their device is ever lost or stolen. Nurse Practitioners should get in the habit of keeping their mobile devices with them at all time. Finally, in the event of the termination of an employee, the employee is responsible for ensuring that their mobile devices are returned to their manager promptly. If the employee does not return the device promptly after being terminated they can prosecuted. Additionally, the SOP outlines to the nurse practitioner their responsibilities in the event of a security breach, including notification of their and manager, IT department, and privacy officer.

Educational Program

Now that policies and procedures related to mobile device use have been established, the next step is to educate the employees about the organization's Standard Operating Procedure. Appendix B, provides a PowerPoint that can be used to train Nurse Practitioners and other clinicians. The first three slides after the introduction in the PowerPoint start by identifying the relevant law. HIPAA requires compliance not only on the organizational level but at the practitioner's level as well, both can be held liable in the event of a breach. It is for this reason that practitioners need to understand the implications associated with HIPAA and HITECH (the legislation that expanded HIPAA). Slide 4 discusses the civil and criminal penalties for failing to comply with the law.

Next, the presentation goes into the definition of PHI provided by HIPAA. Nurse Practitioners need to understand the type of information that they need to protect, everything from names, addresses and account number must be protected under HIPAA. The following

slide illustrates the risks mobile devices present to electronic PHI. Here, Nurse Practitioner should be educated on some of the risks they face when working in the field. The presentation continues by discussing the requirements for protecting PHI named in HIPAA. These include using strong passwords, installing and using encryption and using secure WiFi networks. Finally the presentation ends with a form that should be signed by the Nurse Practitioner and dated attesting to the completion of the training. The law requires that training be conducted annually so organizations should update this training guide continuously and implement it on a recurring basis.

By signing that they have completed the training program, the Nurse Practitioner is agreeing to follow the policies and procedures laid out by the organization. Failure to comply with the SOP will result in disciplinary action or termination.

Questionnaire

Finally, Appendix C provides a questionnaire for the practitioners that partook in the training. The purpose of this questionnaire is to understand the level of comprehension employees have on this topic. Additionally, it allows an organization to gage the overall success of the training program and to understand which areas they need to focus on in future trainings. For example, if the questionnaire is returned with a large portion of wrong answers on what constitutes PHI, the presentation should be modified to account for this shortcoming. Since this is to be implemented annually it is important that the education program be modified regularly to take into consideration new regulation, and weaknesses identified over the course of the year. Successful completion of the training program would commence with the learner achieving an 80% or better on the questionnaire. If the learner scored lower than 80% then they would have

to review the PowerPoint educational program and retake the questionnaire until they have achieved a passing score.

Ongoing Training

The Director on an annual basis will update the SOP and ensure that all staff completes the privacy and security training. Also, any issues or concerns affecting security or the use of mobile devices will be addressed and serve as an educational update throughout the year. The post educational questionnaire and PowerPoint will be updated to reflect any changes in the SOP. New hires will be responsible to successfully complete the training program before using corporate assigned mobile devices. The IT department will work with the director to ensure that the devices used have updated security software and appropriate firewall protection to ensure device security.

Conclusion

Mobile devices are now becoming common place in the healthcare industry, with Nurse Practitioners leading the way in utilization. Nurse Practitioners are among the "digital omnivores" regularly using laptops, tablets and smartphones. Mobile devices greatly facilitate the mobility of Nurse Practitioners working in the field. It allows them to easily access patient records and has been linked to better clinical decision-making. Unfortunately, the added benefits associated with mobile devices are mitigated by a great deal of risk. It is important for these providers to have comprehensive mobile device security/privacy education and review on an annual basis to raise awareness.

In addition, providers need to follow the appropriate steps in the event of a security breach not only to protect the PHI of their patients but to mitigate the financial/legal implications that may arise from the breach. The SOP, training presentation and questionnaire provided, are tools that can be utilized to prevent the risks associated with PHI breaches over mobile devices. It is important to raise awareness that cyber criminals use various electronic means to illegally obtain PHI, as well as the risk associated with simple loss and theft of mobile devices. Therefore, through successful implementation of an SOP, completion of a privacy and security training program Nurse practitioners will be able to safely use their mobile devices to view and transmit PHI in accordance with the law as well as their internal mobile device corporate policy and procedure.

Appendix A

Standard Operating Procedures for Mobile Device Use (SOP)

Purpose:

The purpose of the Nurse Practitioner (NP) standard operating procedures related to Mobile Device/protected health information (PHI) access is to ensure that the access, and the use is secure and within the guidelines of corporate policy as well as in compliance with HITECH and the HIPAA security rule.

Definitions:

NPs are required to provide comprehensive exams and medically manage members in skilled facilities throughout the market. The Nurse practitioners use mobile devices such as laptops, smartphones and tablets to document medical information and access their electronic medical records (PHI).

Policy:

The Nurse practitioner utilizes mobile devices to access the PHI system in contracted facilities to review and enter information pertaining to patient medical records. The authorization to access and use the PHI, as well as the security of the PHI credentials is critical to compliance, patient

record integrity, and overall reputation of the organization. This policy/procedure will outline the specific requirements pertaining to the PHI mobile device system access, and security requirements.

Process:

PHI Access Request Process

Steps for granting an employee access to PHI:

- Manager review of this policy/procedure
- Human Resources Access request for the PHI access, including role and business need
- The individual will be notified upon approval by email from IT security.
- The PHI access and security application will be retained pursuant to record retention policy/procedure

General PHI Access Security Requirements

Access to PHI systems must be authenticated through a process that includes, at a minimum:

- Issuance of unique PHI access credentials that enable each PHI User's activity to be identified and tracked.
- The prompt removal of PHI User access privileges for users whose employment or contracted service with the appropriate management company has ended.
- Assignment of PHI permission levels associated with the PHI User's business need for PHI access.

PHI Users must protect their PHI access credentials from other individuals, PHI applicants, or PHI users by:

- Reasonably protecting their PHI access credentials from disclosure
- Not sharing PHI access credentials
- Not allowing others to view PHI access credentials

Mobile Device Users while logged into the PHI under their access credentials may not allow other individuals, PHI applicants, or PHI Users to:

- View PHI information while logged into the PHI
    - Exception- patients may be permitted to view their PHI records
- Make any entries in the PHI
- Complete any other function (e.g. print, run reports, etc.)
- Access, transmit, or receive health information via an unsecured Wi-Fi network
- Must use encryption to protect information and communication

PHI Mobile device interfaces (iPads, smartphones, Laptops, Monitors etc.) must be physically located or positioned in such a manner as to minimize the risk of access by unauthorized users by:

- Positioning the viewing screen away from windows, walkways, or persons waiting in reception, public, or other areas.
- Using a privacy screen
- Locking the device when not in use
- Maintaining physical possession of the device at all times.

PHI Users are required to immediately notify their direct supervisor and the privacy officer when any of the following occurs:

- PHI access credentials have been disclosed, lost or otherwise released to others
- Mobile device is lost or stolen

Monitoring

All mobiles devices are subject to compliance auditing against policy/procedure, as well as government compliance.

The following actions will be taken for violations:

- The PHI User and direct supervisor will be immediately notified.
- The PHI User's permission level will be immediately changed to "read only"
- The PHI User's direct supervisor will be responsible for ensuring the completion of any outstanding items pending in the PHI.
- Employed PHI Users will be referred to Compliance, Legal, and Human Resources for disciplinary measures up to and including termination.
- Non- employed PHI Users will be referred to Compliance/Legal for investigation and disposition.

Termination-Voluntary or Involuntary

- Manager is responsible to notify IT of termination and put in a request through HS access.
- Employees are responsible to return immediately all mobile devices in their possession to the IT department.

Appendix B

(see powerpoint)

Appendix C

Mobile Devices: Security and Privacy Questionnaire

1.) When using a mobile device to work remotely, you must do all the following except:
- a.) Lock Screen when not in use
- b.) Use a privacy screen when using a mobile device in public areas
- c.) Change default administrator passwords and usernames
- d.) Use a virtual VPN to connect to your organization's private network

2.) When creating a password, the password should include:
- a. Capital letters
- b. Lower Case Letter
- c. Special Characters (e.g. $, !, and @)
- d. More than 8 letters and characters
- e. All of the above

3.) Criminal Penalties for a person who knowingly obtains or discloses identifiable health information in violation of HIPAA faces a fine of $50, 000 and up to one year in prison.
- a.) True
- b.) False

4.) When using your mobile device in a public space, you should do the following EXCEPT:
- a.) Use an unsecured WIFI
- b.) Use a secure browser connection
- c.) Use strong passwords
- d.) Always keep your laptop, cellphone, iPad with you at all times.
- e.) All of the above

5.) All the following activities make a device vulnerable for attack except:
- a.) Blocking software downloads
- b.) Visiting a malicious website
- c.) Linking into different communication networks
- d.) Stolen or lost devices can allow access of authorized persons to access PHI

6.) All of the following are considered mobile devices except:

a.) Smartphones
b.) Laptops
c.) Tablets
d.) Fax machines
e.) USB

7.) HIPAA rules apply to the following covered entities:
a.) Health Care provider
b.) A health plan
c.) A health care billing company
d.) All of the above

8.) HIPAA privacy rule contains all the following except:
a.) Provides federal protection for individually identifiable health information by covered entities and business associates
b.) Permits the disclosure of health information needed for patient care
c.) Gives patient's rights with respect to the disclosure of their health information.
d.) Allows providers to share PHI with other providers as requested

9.) Protected Health information includes all of the following except:
a.) A patient's address
b.) Social security number
c.) Pharmacy name
d.) Past, present and future payment provisions of health care

10.) Having a strong password is key to security, a health care provider should do the following:
a.) Change passwords frequently
b.) Do not reuse passwords
c.) Change default settings
d.) All of the above

11.) A virtual private network or VPN is the preferred network to keep PHI secure, an example of this includes:
a.) Websites that ask for username and password
b.) A company or hospital that has Https: listed in the browser
c.) MSN Hotmail account
d.) A public WIFI in a long term care facility

12.) Encryption is a method of converting an original message of regular text into numbers:
a.) True
b.) False

13.) The number one cause of PHI breaches on mobile devices is caused by the following;
a.) Loss

b.) Theft
c.) Unauthorized disclosure
d.) Hacking

14.) Once a mobile device is no longer being used, the health care provider should do the following:
a.) Take the device to a recycling center
b.) Install a new operating system and allow staff to use as needed
c.) Remove old hard drives and either destroy or wipe them permanently to remove all data prior to disposal.
d.) Use the device for non-medical purposes

15.) A colleague is at a conference and asks you to email a patient's lab results so he can review them. In order to be HIPAA compliant, you do the following:
a.) Knowing that he has a password on his email account, you email the results as requested.
b.) You ask him for the hotel fax number and fax the lab results with a cover page-attention: Dr. Smith
c.) You determine he has access to an encrypted email, so you send the results to this email address.
d.) None of the above

References

Ackerman, M. (2010). Meaningful Use? *The Journal of Medical Practice Management, 25*(5), 320-321. Retrieved from ProQuest Central.

Agrawal, S., Budetti, C. (2012). Physician Medical Identity Theft. JAMA; 307: 459-460.

Bandura, A. (1986). Social Foundations of Thought and Action. New Jersey: Prentice Hall

Bandura, A. (1997). Analysis of self-efficacy theory of behavioral change. *Cognitive Therapy and Research*. 1(4), 287-304.

Barrett, C. (2011), Healthcare providers may violate HIPAA by using Mobile devices to Communicate with patients, ABA Health esource, volume 8, number 2.

Cucoranu IC, Parwani AV, West AJ, et al. Privacy and security of patient data in the pathology laboratory. *J Pathol Inform*. 2013;4:4.

Dolan, P. (2011), Doctors driving IT development with their mobile device technology choices, amednews.com.

Fisher, M. (2015, March 5). Training: A Necessary and Essential Part of HIPAA Compliance. Retrieved March 5, 2015, from http://www.hitechanswers.net/training-a-necessary-and-essential-part-of-hipaa-compliance/

Herold, R. (2011), 10 risk reducing actions for mobile HIPAA/HITECH compliance, mobile healthcare today.com

Hickney, Andrew (2007). Mobile security is end user and IT responsibility, Computerweekly.com

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191)

The HIPAA Privacy Rule and electronic health information exchange in a networked environment: accountability (2009).

Department of Health & Human Services (2007). HIPAA Security Series. Center for Medicare and Medicaid Services, volume 2, paper 4.

Kolbasuk, McGee M. (2011). How secure are your clinicians' mobile devices. Retrieved March 26, 2015, from http://www.informationweek.com/news/healthcare/mobile-wireless/231903089.

Levingston SA. Opportunities in physician electronic health records: a road map for vendors. *Bloomberg Government*; 2012.

Mangan, D. (2014, April 24). Patient Privacy Payouts! Coughing up big bucks for missing patient health data. Retrieved March 26, 2015, from http://www.cnbc.com/id/101607607

McCarthy, K. (2014). Study: Majority of healthcare data breaches due to theft. Retrieved March 27, 2015.

McDavid, J. (2013). HIPAA Risk Is Contagious: Practical Tips to Prevent Breach. The Journal of Medical Practice Management, 29(1), 53-55. Retrieved March 25, 2015, from ProQuest Central.

Myers, E. (2015, March 13). Meaningful Use Attestations Up Slightly as March 20 Deadline Nears - iHealthBeat. Retrieved March 27, 2015.

Taitsman, J., Grim, C., Shantanu, A. (2013). Protecting Patient Privacy and Data Security. N Eng J Medicine, 368; 977-978.

Torrieri, M. (2011) Lowering mobile device security risks for patients, physician practice.

Ventola, C. (2014). Mobile Devices and Apps for Health Care Professionals: Uses and Benefits. *Pharmacy and Therapeutics, 39*(5), 356-364. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/

Walker, D. (2014). Integrating privacy and security into your practice. SC magazine.

Yu, E. (2013). HIPAA Privacy and Security: Analysis of Recent Enforcement Actions. The Journal of Health Care Compliance, 15(5), 59-61. Retrieved March 26, 2015, from ProQuest Central.